

REMARKS

Claims 1, 5, 11-13, 16, 27, 36, 37, 41 and 42 are amended. Claims 4, 14, 17, 18 and 34 are canceled. Claims 1-3, 5-13, 15, 16, 19-33 and 35-42 remain in the application. In view of the following remarks, Applicant respectfully requests withdrawal of the application and forwarding of the application on to issuance.

The Rejections

Claims 1, 5, 11-12, 37-42 stand rejected under 35 U.S.C §102(e) as being anticipated by U.S. Patent No. 6,678,733 to Brown et al. (hereinafter "Brown").

Claim 2 stands rejected under 35 U.S.C §103(a) as being obvious over Brown in view of U.S. Patent No. 6,070,243 to See et al. (hereinafter "See") and U.S. Patent No. 6,237,095 to Curry et al. (hereinafter "Curry").

Claim 3 stands rejected under 35 U.S.C §103(a) as being obvious over Brown in view of See.

Claims 4 and 6-10 stand rejected under 35 U.S.C §103(a) as being obvious over Brown in view of U.S. Patent No. 6,609,954 to Moreau.

Claim 8 stands rejected under 35 U.S.C §103(a) as being obvious over Brown in view of Moreau and See.

Claims 13, 15 and 16-18 stand rejected under 35 U.S.C §103(a) as being obvious over Brown in view of U.S. Patent No. 6,584,564 to Olkin et al. (hereinafter "Olkin").

Claim 14 stands rejected under 35 U.S.C §103(a) as being obvious over Brown in view of Olkin and See.

1 Claims 19, 24 and 26 stand rejected under 35 U.S.C §103(a) as being obvious
2 over Brown in view of U.S. Patent No. 6,115,376 to Sherer et al. (hereinafter
3 "Sherer").

4 Claims 20-22 stand rejected under 35 U.S.C §103(a) as being obvious over
5 Brown in view of Sherer and Olkin.

6 Claim 23 stands rejected under 35 U.S.C §103(a) as being obvious over
7 Brown in view of Sherer, Olkin and U.S. Patent No. 6,304,969 to Wasserman et al.
8 (hereinafter "Wasserman").

9 Claim 25 stands rejected under 35 U.S.C §103(a) as being obvious over
10 Brown in view of Sherer and U.S. Patent No. 5,937,068 to Audebert.

11 Claims 27, 28, 30, 31, 33, 35 and 36 stand rejected under 35 U.S.C §103(a) as
12 being obvious over Brown in view of Audebert and U.S. Patent No 6,295,361 to
13 Kandansky et al. (hereinafter "Kandansky").

14 Claim 29 stands rejected under 35 U.S.C §103(a) as being obvious over
15 Brown in view of Audebert, Kandansky and Wasserman.

16 Claim 32 stands rejected under 35 U.S.C §103(a) as being obvious over
17 Brown in view of Audebert, Olkin and Biran.

18 Claim 34 stands rejected under 35 U.S.C §103(a) as being obvious over
19 Brown in view of Audebert, Kandansky and See
20

21 The Claims

22 Claim 1 has been amended and recites a method of updating keys that
23 decrypt login tickets that log a user into multiple sites, the method comprising [added
24 language appears in bold italics]:
25

- generating a first key having a first version number;
- providing tickets encoded consistent with the first key, the ticket having a version number corresponding to the first version number;
- generating a second key having a second version number; and when the second key becomes current at a site, providing tickets encoded consistent with the second key, the ticket having a version number corresponding to the second version number;
- wherein *said keys comprise key data and executable code for decrypting tickets.*

In making out the rejection of this claim, the Office argues that it is anticipated by Brown. Applicant respectfully disagrees, particularly in view of the amendment made above. Specifically, this claim has been amended to incorporate the subject matter of its formerly dependent claim 4. The Office rejected claim 4 using the combination of Brown and Moreau. In relying on Moreau, the Office argued that Moreau teaches the use of a key in the form of an executable, citing to column 2, lines 23-32 for support.

Applicant disagrees with the Office's interpretation of Moreau. Specifically, the passage cited by the Office simply states as follows: "[w]ith the proprietary approach, the security is based on...the obscure embedding of such cryptographic key in the executable portion of a software application...." The claim, on the other hand, recites that "said keys *comprise...executable code for decrypting tickets.*" Thus, the keys themselves comprise the code for decrypting tickets. Moreau, on the other hand, simply teaches embedding a key in an executable portion of a software application. The cited passage does not teach or suggest a key that itself comprises executable code.

Accordingly, the Office has failed to establish a *prima facie* case of obviousness and this claim is allowable.

1 **Claims 2 and 3** depend from claim 1 and are allowable as depending from
2 an allowable base claim. These claims are also allowable for their own recited
3 features which, in combination with those recited in claim 1, are neither disclosed
4 nor suggested in the references of record, either singly or in combination with one
5 another. In addition, given the allowability of claim 1, the further rejection of
6 claim 2 over the combination with See and Curry is not seen to add anything of
7 significance.

8 **Claim 5** has been amended and recites a computer readable medium having
9 instructions stored thereon for causing a computer to perform a method of updating
10 keys that decrypt login tickets that log a user into multiple sites, the method
11 comprising [added language appears in bold italics]:

- 12 • generating a first key having a first version number;
- 13 • providing tickets encoded consistent with the first key, the ticket
14 having a version number corresponding to the first version number;
- 15 • generating a second key having a second version number; and
- 16 • when the second key becomes current at a site, providing tickets
17 encoded consistent with the second key, the ticket having a version
18 number corresponding to the second version number;
- 19 • wherein ***said keys comprise key data and executable code for***
20 ***decrypting tickets.***

21 As noted above, neither Brown nor Moreau disclose or suggest any such
22 subject matter. Accordingly, this claim is allowable.

23 **Claim 6** recites a method of generating keys that decrypt login tickets that
24 log a user into multiple sites, the method comprising:

- 25 • generating ***a first key in the form of an executable*** having a first
version number;

- generating *a second key in the form of an executable* having a second version number; and
- providing an indication to a login server identifying which key is current for each site such that the tickets are properly encoded.

In making out the rejection of this claim, the Office argues that Brown discloses all features of the claim except for a key comprising key data and executable code for decrypting tickets. The Office then relies on Moreau as noted above. Applicant respectfully traverses the Office's rejection. Specifically, Moreau does not disclose or suggest a key *in the form of an executable*. Accordingly, the Office has not established a *prima facie* case of obviousness and this claim is allowable.

Claims 7 and 8 depend from claim 6 and are allowable as depending from an allowable base claim. These claims are also allowable for their own recited features which, in combination with those recited in claim 6, are neither disclosed nor suggested in the references of record, either singly or in combination with one another. In addition, given the allowability of claim 6, the rejection of claim 8 over the combination with See is not seen to add anything of significance.

Claim 9 recites a computer readable medium having instructions stored thereon for causing a computer to perform a method of generating keys that decrypt login tickets that log a user into multiple sites, the method comprising:

- generating *a first key in the form of an executable* having a first version number;
- generating *a second key in the form of an executable* having a second version number; and
- providing an indication to a login server identifying which key is current for each site such that the tickets are properly encoded.

1
2 The Office rejects this claim and uses the same arguments as were used in
3 making out the rejection of claim 6. Applicant respectfully notes that neither
4 Brown, Moreau nor See disclose or suggest keys in the form of executables as
5 contemplated in this claim. Accordingly, for at least this reason, the Office has
6 failed to establish a *prima facie* case of obviousness and this claim is allowable.

7 Claim 10 recites a system that generates keys that decrypt login tickets that
8 log a user into multiple sites, the system comprising:

- 9
- 10 • a key generator that generates *a first key in the form of an executable*
 - 11 *having a first version number and generates a second key in the form*
 - 12 *of an executable having a second version number; and*
 - 13 • means for providing information to a login server identifying which
 - 14 key is current for each site such that the tickets are properly encoded.

15 The Office rejects this claim and uses the same arguments as were used in
16 making out the rejection of claim 6. Applicant respectfully notes that neither
17 Brown, Moreau nor See disclose or suggest keys in the form of executables as
18 contemplated in this claim. Accordingly, for at least this reason, the Office has
19 failed to establish a *prima facie* case of obviousness and this claim is allowable.

20 Claim 11 has been amended and recites a method of updating keys that
21 decrypt login tickets that log a user into multiple sites, the method comprising [added
22 language appears in bold italics]:

- 23
- 24 • generating a new key with an incremented version number;
 - 25 • sending the new key to a partner site for use in decoding tickets with
the incremented version number;
 - updating key and version information for a login server; and

- generating tickets decodable by the new key when an indication that a key having a previous version number has expired;
- wherein *said keys comprise key data and executable code for decrypting tickets.*

In making out the rejection of this claim, the Office argues that its subject matter is anticipated by Brown. Applicant disagrees, particularly in view of the amendment that has been made. As such, this claim is allowable.

Claim 12 has been amended and recites a computer readable medium having instructions stored thereon for causing a computer to perform a method of updating keys that decrypt login tickets that log a user into multiple sites, the method comprising [added language appears in bold italics]:

- generating a new key with an incremented version number;
- sending the new key to a partner site for use in decoding tickets with the incremented version number;
- updating key and version information for a login server; and
- generating tickets decodable by the new key when an indication that a key having a previous version number has expired;
- wherein *said keys comprise key data and executable code for decrypting tickets.*

In making out the rejection of this claim, the Office argues that its subject matter is anticipated by Brown. Applicant disagrees, particularly in view of the amendment that has been made. As such, this claim is allowable.

Claim 13 has been amended and recites a method of updating a key used to decrypt tickets used to log into a site, the method comprising [added language appears in bold italics]:

- receiving an updated key with a new version number;

- setting a time for an old current key having an old version number to expire;
- making the updated key the current key;
- wherein *at least one of said keys comprise executable code for making the updated key the current key.*

In making out the rejection of this claim, the Office argues that the claim is rendered obvious over Brown in view of Olkin. Applicant respectfully disagrees particularly in view of the amendment in the present claim. More specifically, this claim has been amended to recite that at least one of the keys comprise executable code for making the updated key the current key. This feature is entirely missing from Brown, Olkin and Moreau. As such, the Office has failed to establish a *prima facie* case of obviousness. Accordingly, this claim is allowable.

Claim 15 depends from claim 13 and is allowable as depending from an allowable base claim. This claim is also allowable for its own recited features which, in combination with those recited in claim 13, are neither disclosed nor suggested in the references of record, either singly or in combination with one another.

Claim 16 has been amended and recites a computer readable medium having instructions stored thereon for causing a computer to perform a method of updating a key used to decrypt tickets used to log into a site, the method comprising [added language appears in bold italics]:

- receiving an updated key with a new version number;
- setting a time for an old current key having an old version number to expire;
- making the updated key the current key;
- wherein *wherein at least one of said keys comprise executable code for making the updated key the current key.*

1
2 In making out the rejection of this claim, the Office argues that Brown
3 discloses all of the features of the claim except for setting a time for an old current
4 key having an old version to expire. The Office then relies on Olkin to supply this
5 missing feature and argues that the claim is obvious in view of these references.

6 Applicant has amended this claim to recite that at least one of the keys
7 comprise executable code for making the updated key the current key. As noted
8 above, none of the references cited by the Office disclose or suggest this feature. As
9 such, this claim is allowable.

10 Claim 19 recites a method of managing keys used to decrypt tickets for
11 logging onto a site, the method comprising:

- 12
- 13 • receiving a first key with a first version number;
 - 14 • encrypting the first key using a hardware address;
 - 15 • changing a current key variable to the first version number;
 - 16 • receiving a new key with an incremented version number;
 - 17 • encrypting the new key using a hardware address; and
 - 18 • identifying the new key as the current key.

19 In making out the rejection of this claim, the Office argues that Brown
20 discloses all of the features of the claim except for encrypting the first key and the
21 new key using a hardware address. The Office then relies on Sherer for this feature,
22 citing to column 7, lines 35-37, and argues that the combination of these references
23 renders the subject matter of this claim obvious. Applicant respectfully disagrees
24 and traverses the Office's rejection.

25 In making out the rejection of this claim, the Office appears to argue, citing to
the Specification on page 10, lines 2-4, that the recited feature "encrypting the new

1 key using a hardware address" simply refers to storing the key using a piece of
2 information that is specific to the physical machine, such as the MAC address of the
3 first network card. Applicant respectfully disagrees and refers the Office to page 11,
4 lines 22-23 which states: "[k]eydata contains the actual keys, encrypted in the
5 HMAC of the machine."

6 Sherer simply discloses that a so-called "star interconnection device stores, or
7 otherwise has access to a certificate binding a MAC address on a port to a public
8 key." This in no way discloses or suggests encrypting a new key using a hardware
9 address.

10 Accordingly, for at least this reason, the Office has failed to establish a *prima*
11 *facie* case of obviousness and this claim is allowable.

12 **Claims 20-25** depend from claim 19 and are allowable as depending from
13 an allowable base claim. These claims are also allowable for their own recited
14 features which, in combination with those recited in claim 19, are neither disclosed
15 nor suggested in the references of record, either singly or in combination with one
16 another. In addition, given the Office's failure to establish a *prima facie* case of
17 obviousness with respect to claim 19, the further rejections of claims 20-22 over
18 Olkin, of claim 23 over Olkin and Wasserman, and claim 28 over Audebert are not
19 seen to add anything of significance.

20 **Claim 26** recites a computer readable medium having instructions stored
21 thereon for causing a computer to perform a method of managing keys used to
22 decrypt tickets for logging onto a site, the method comprising:

- 23
- 24 • receiving a first key with a first version number;
 - 25 • *encrypting the first key using a hardware address;*
 - changing a current key variable to the first version number;

- receiving a new key with an incremented version number;
- *encrypting the new key using a hardware address*; and
- identifying the new key as the current key.

In making out the rejection of this claim, the Office argues that Brown discloses all of the features of the claim except for encrypting the first key and the new key using a hardware address. The Office then relies on Sherer for this feature and argues that the combination of these references renders the subject matter of this claim obvious. Applicant respectfully disagrees and traverses the Office's rejection.

As noted above, Sherer neither discloses nor suggests encrypting keys using a hardware address. Accordingly, for at least this reason, the Office has failed to establish a *prima facie* case of obviousness and this claim is allowable.

Claim 27 has been amended and recites a method of updating keys used to decrypt tickets used to log into multiple sites on a network, the method comprising [added language appears in bold italics]:

- generating a new key with a new version number to take the place of an old key with an old version number;
- storing the new key on a site to be logged into by a user;
- changing a current key indication to the new key;
- allowing current logged in users to continue using the old key; and
- redirecting new users to a login server to obtain a ticket consistent with the new key;
- *wherein keys are generated in an executable form which includes key information as well as code for decrypting tickets using the key information.*

This claim has been amended to incorporate the subject matter of claim 34. In making out the rejection of claim 34, the Office argues that Brown, Audebert and Kandansky teach all of the features of this claim except for generating keys in an

1 executable form which includes key information as well as code for decrypting
2 tickets using the key information. The Office then relies on See for the missing
3 subject matter and argues that the subject matter of claim 34 is obvious in view of
4 these references. Applicant respectfully disagrees and traverses the Office's
5 rejection.

6 Applicant respectfully submits that the Office has mischaracterized See.
7 Specifically, the excerpt cited by the Office simply states that an agent 400 is
8 configured with an address of a device, an address of a basic server and an
9 authentication key for server 320. This excerpt does not state or even imply that the
10 key is generated in executable form which includes key information as well as code
11 for decrypting tickets using the key information.

12 Accordingly, for at least this reason, the Office has failed to establish a *prima*
13 *facie* case of obviousness and this claim is allowable.

14 Claims 28-33 and 35 depend from claim 27 and are allowable as
15 depending from an allowable base claim. These claims are also allowable for their
16 own recited features which, in combination with those recited in claim 27, are
17 neither disclosed nor suggested in the references of record, either singly or in
18 combination with one another. In addition, in view of the Office's failure to
19 establish a *prima facie* case of obviousness with respect to claim 27, the rejections
20 of claim 29 over the combination with Wasserman, and of claim 32 over Olkin
21 and Biran is not seen to add anything of significance.

22 Claim 36 has been amended and recites a computer readable medium
23 having instructions stored thereon for causing a computer to perform a method of
24 updating keys used to decrypt tickets used to log into multiple sites on a network, the
25 method comprising [added language appears in bold italics]:

- generating a new key with a new version number to take the place of an old key with an old version number;
- storing the new key on a site to be logged into by a user;
- changing a current key indication to the new key;
- allowing current logged in users to continue using the old key; and
- redirecting new users to a login server to obtain a ticket consistent with the new key,
- *wherein the keys comprise key data and executable code for decrypting tickets.*

The Office rejects this claim and makes arguments that are the same as those made with respect to claim 27. For all of the reasons set forth with respect to the Office's failure to establish a *prima facie* case of obviousness in the rejection of claim 27, this claim is allowable.

Claim 37 has been amended and recites a method of logging on to multiple sites, the method comprising [added language appears in bold italics]:

- sending a first login ticket to a desired site, wherein the login ticket is encrypted to be decoded by a first key having a first version number;
- receiving an indication that the first key has expired;
- obtaining a second login ticket from an authentication server, wherein the second login ticket is encrypted consistently with a new key having a second version number; and
- sending the second login ticket to the site to log into the site;
- *wherein the keys comprise key data and executable code for decrypting tickets.*

In making out the rejection of this claim, the Office argues that it is anticipated by Brown. Applicant respectfully disagrees, particularly in view of the amendment made above. Accordingly, for at least this reason, this claim is allowable.

1 **Claims 38-40** depend from claim 37 and are allowable as depending from
2 an allowable base claim. These claims are also allowable for their own recited
3 features which, in combination with those recited in claim 37, are neither disclosed
4 nor suggested in the references of record, either singly or in combination with one
5 another.

6 **Claim 41** has been amended and recites a computer readable medium
7 having instructions stored thereon for causing a computer to perform a method of
8 logging on to multiple sites, the method comprising [added language appears in bold
9 italics]:

- 10 • sending a first login ticket to a desired site, wherein the login ticket is
- 11 encrypted to be decoded by a first key having a first version number;
- 12 • receiving an indication that the first key has expired;
- 13 • obtaining a second login ticket from an authentication server, wherein
- 14 the second login ticket is encrypted consistently with a new key having
- 15 a second version number; and
- 16 • sending the second login ticket to the site to log into the site;
- 17 • wherein *the keys comprise key data and executable code for*
- 18 *decrypting tickets.*

19 In making out the rejection of this claim, the Office argues that it is
20 anticipated by Brown. Applicant respectfully disagrees, particularly in view of the
21 amendment made above. Accordingly, this claim is allowable.

22 **Claim 42** has been amended and recites an encrypted ticket for use in
23 logging on to a website, the ticket comprising [amended language appears in bold
24 italics]:

- 25 • an unencrypted version number corresponding to a key version
 number stored on the website; and

- an encrypted string identifying the website and information, which when decrypted using the key having the same version number authenticates the user for logging the user into the website;
- wherein *the key comprises executable code for decrypting tickets.*

In making out the rejection of this claim, the Office argues that it is anticipated by Brown. Applicant respectfully disagrees, particularly in view of the amendment made above. Accordingly, this claim is allowable.

Conclusion

Applicant respectfully submits that all of the claims are in condition for allowance. If the Office's next anticipated action is to be anything other than issuance of a Notice of Allowability, Applicant respectfully requests a telephone call for the purpose of scheduling an interview.

Dated: 6/25/04

Respectfully Submitted,

By. 

Lance R. Sadler
Reg. No. 38,605
(509) 324-9256